UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,423	03/29/2001	Michael S. Ripley	42390P10855	9405

8791 7590 01/09/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
LEE, CHI CHUNG	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 01/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,423	RIPLEY ET AL.	
	Examiner	Art Unit	
	Chi-Chung E Lee	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *16 October 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-26 are remain rejected under 35 U.S.C. 103(a) as being unpatentable over Natsume et al in view of Miyauchi et al (US 6,272,225 B1).

As per claims 1, 5, Natsume discloses a system comprising:

an encryption subsystem [see figure 2] to encrypt data accessed from a storage medium containing a key distribution data block (i.e. master key 7, see figure 2] using an encryption bus key (i.e. title key) prior to transmitting the encrypted data [see page 8 lines 18-21] via a data bus (i.e. PC bus 7, see figure 5). Natsume discloses the encryption bus key (i.e. encrypted title key) is derived based on at least a portion of the key distribution data block (i.e. master key), at least one device key (i.e. disc key) assigned to said encryption subsystem [see page 10 lines 1-16]. Natsume discloses the content scramble process in figure 2 and use the title key instead of the encrypted title to encrypt the AV contents. It would have been obvious to employ the encrypted title (i.e. encryption bus key) to scramble the data in the system of Natsume because it pass the encrypted title key to the DVD and the encrypted title key can be decrypted only by the master key and disc key.

Natsume does not expressly disclose a number generator to generator a nonce and use it to generate the bus key.

Miyauchi discloses a random generator 400 [see figure 1] to generate a nonce (i.e. random number Kr, see figure 1) and output it to the random key encryption unit 310 [see column 4 lines 3-14].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to add the random generator within the system of Natsume to generate a nonce and use it to generate the bus key.

One of ordinary skill in the art would have been motivated to add an extra layer of key management scheme inclusive of the random key (i.e. nonce) in the system of Natsume so as to protect data privacy and to recover the encrypted data.

As per claims 2, 6, 8, 10, Natsume discloses the system comprising:

a decryption subsystem [see figure 5] coupled to said data bus to decrypt data received over the data bus using an decryption bus key derived based on at least a portion of the key distribution data block (i.e. master key), at least one device key (i.e. disc key) assigned to said encryption subsystem [see page 10 lines 1-16].

Natsume does not expressly disclose a number generator to generator a nonce and use it to generate the decryption bus key.

Miyauchi discloses a random generator 400 [see figure 1] to generate a nonce (i.e. random number Kr, see figure 1) and output it to the random key encryption unit 310 [see column 4 lines 3-14].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to add the random generator within the system of Natsume to generate a nonce and use it to generate the decryption bus.

One of ordinary skill in the art would have been motivated to add an extra layer of key management scheme inclusive of the random key (i.e. nonce) in the system of Natsume so as to protect data privacy and to recover the encrypted data.

As per claim 3, Natsume discloses the encryption subsystem comprises:

a) a processing logic (i.e. CSS management organization, see page 10 lines 14-16) to process at least a portion of the key distribution data block read from the storage medium (i.e. DVD) using the device key (i.e. disc key) to compute a media key (i.e. title key, see page 10 lines 9-16);

b) an encryption logic (i.e. content encryption 4, see figure 1) to encrypt data accessed from said storage medium using said encryption bus key (i.e. encrypted title key, see page 10 lines 1-3).

Natsume does not expressly disclose an one-way function to generate the encryption bus key based on the media key and a nonce generated by the number generator.

Miyauchi discloses a random generator 400 [see figure 1] to generate a random number Kr (i.e. nonce, see figure 1) and hashing unit 100 (i.e. one-way function, see figure 1) and output them to the concatenating unit 510 [see column 4 lines 3-24].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to add the random generator to generate a nonce and hashing unit within the system of Natsume and use the nonce and the disc key to generate the encryption bus key.

One of ordinary skill in the art would have been motivated to add an extra layer of key management scheme inclusive of the random key (i.e. nonce), hashing unit and concatenating unit in the system of Natsume so as to protect data privacy and to recover the encrypted data.

As per claim 4, Natsume discloses the decryption subsystem comprises:

a) a processing logic (i.e. CSS management organization, see page 10 lines 14-16) to process at least a portion of the key distribution data block read from the storage medium (i.e. DVD) using the device key (i.e. disc key) to compute a media key (i.e. title key, see page 10 lines 9-16);

b) a decryption logic (i.e. descramble 9, see figure 5) to decrypt data accessed from said storage medium using said encryption bus key (i.e. encrypted title key, see page 10 lines 1-3).

Natsume does not expressly disclose an one-way function to generate the decryption bus key based on the media key and a nonce generated by the number generator.

Miyauchi discloses a random generator 400 [see figure 1] to generate a random number Kr (i.e. nonce, see figure 1) and hashing unit 100 (i.e. one-way function, see figure 1) and output them to the concatenating unit 510 [see column 4 lines 3-24].

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to add the random generator to generate a nonce, the hashing unit and the concatenating unit within the decryption subsystem of Natsume and use the nonce and the disc key to generate the decryption bus key.

One of ordinary skill in the art would have been motivated to add an extra layer of key management scheme inclusive of the random key (i.e. nonce), hashing function and concatenating unit in the system of Natsume so as to protect data privacy and to recover the encrypted data.

As per claim 7, Natsume discloses the encryption subsystem is implemented in a storage device (i.e. DVD player, see figure 1) capable of accessing data from a storage medium (i.e. DVD) and said decryption subsystem is implemented in a host device (i.e. computer, see figure 5) capable of retrieving data from said storage device [see page 13 lines 10-24].

As per claim 9, Natsume discloses the storage medium is selected form a digital versatile disc (DVD) [see figure 1 and page 5 lines 9-22].

As per claims 11-17, the claimed steps corresponds to the functions of the elements of the apparatus claims 1-10, which has been rejected above, and thus rejected with the same reason applied thereto.

Claims 18-26 have similar limitations as claims 1-10; therefore, they are rejected under the same rationale.

Response to Amendment

Applicant has argued that the present invention requires that the combination of Natsume and Miyauchi fail to teach deriving an encryption bus key. The examiner disagrees. Natsume teaches the encrypted title key (i.e. encryption bus key) is derived from master key, disc key, and master key, see page 8 line 6-14) and Miyauchi teaches the one-time pad key.

Applicant has argued that the figure 3 of Natsume is no way teaches or suggests an encryption subsystem. However, Natsume teaches the encryption procedures in figure 2 for scrambling the AV contents.

The **totality of the prior art must be considered**, and proceeding contrary to accepted wisdom in the art is evidence of nonobviousness. In re Hedges, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986) (Applicant's claimed process for sulfonating diphenyl sulfone at a temperature above 127°C was contrary to accepted wisdom because the **prior art as a whole suggested** using lower temperatures for optimum results as evidenced by charring, decomposition, or reduced yields at higher temperatures.). Furthermore, "[k]nown disadvantages in old devices which would naturally discourage search for new inventions may be taken into account in determining obviousness." United States v. Adams, 383 U.S. 39, 52, 148 USPQ 479, 484 (1966).

Applicant has argued that the "title key" taught by Natsume does not serve to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus. In

Response: The examiner disagrees. Natsume discloses the AV contents obtained as results of MPEP compression (i.e. storage medium) are scrambled using the title key [see page 10 lines 1-3]. Natsume also discloses the encrypted title key is stored in the sector region on the disc. It's inherent in the system of Natsume to use the encrypted title key to access the storage medium [see page 10 lines 5-7].

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chi-Chung E Lee whose telephone number is 703-306-4153. The examiner can normally be reached on 8 am - 6 pm, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Chi-Chung Lee
12/31/2003

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100